

确认 Catalyst 5000 EARL 版本和其它常见 EARL 问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[什么是 EARL ？](#)

[从 CLI 中确定 EARL 版本](#)

[从零件号码表中确定 EARL 版本](#)

[模块化 Supervisor Catalyst 5000 系列 Supervisor](#)

[固定配置 Catalyst 5000 系列交换机](#)

[通过 SNMP 确定 EARL 版本](#)

[为何只有 Catalyst 5000 EARL 1 版本受影响？](#)

[如果网络中没有 STP 冗余，是否仍应升级？](#)

[802.1x 的漏洞对 Catalyst 4000 和 6000 没有影响](#)

[Windows 2000 对 802.1x 的支持](#)

[相关信息](#)

简介

本文档解决 Catalyst 5000 交换机的 802.1x 漏洞问题。本文档还包括如何确定 Catalyst 5000 EARL 版本。有关 802.1x 漏洞的详细信息，请参阅以下安全建议：

<http://www.cisco.com/warp/public/707/cisco-sa-20010413-cat5k-8021x.shtml>

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

什么是 EARL ？

编码地址识别逻辑(EARL)是一个集中处理引擎，用于根据Catalyst 5000 Supervisor引擎上的MAC地址学习和转发数据包。EARL存储VLAN、MAC地址和端口关系。这些关系用于在硬件中制定交换决策。

从 CLI 中确定 EARL 版本

要从命令行界面(CLI)确定EARL版本，请从Supervisor发出**show module**命令。以下是示例：

```
Console (enable) sh mod
Mod Module-Name Ports Module-Type Model Serial-Num Status
-----
1 2 100BaseFX MM Supervis WS-X5506 005441962 ok
2 48 10BaseT Ethernet WS-X5012A 010308246 ok
3 48 10BaseT Ethernet WS-X5012A 010308178 ok
4 24 3 Segment 100BaseTX E WS-X5223 005389389 ok
5 12 100BaseFX MM Ethernet WS-X5201R 008951252 ok

Mod MAC-Address(es) Hw Fw Sw
-----
1 00-e0-f9-d6-64-00 to 00-e0-f9-d6-67-ff 1.0 2.2(2) 4.2(1)
2 00-90-6f-6e-75-c0 to 00-90-6f-6e-75-ef 1.0 4.2(1) 4.2(1)
3 00-90-6f-6e-5a-f0 to 00-90-6f-6e-5b-1f 1.0 4.2(1) 4.2(1)
4 00-e0-b0-fb-0a-29 to 00-e0-b0-fb-0a-2b 1.0 2.2(1) 4.2(1)
5 00-60-2f-39-3d-d4 to 00-60-2f-39-3d-df 1.1 4.1(1) 4.2(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1 EARL 1+ WS-F5511 0005442554 1.0
```

上面从Supervisor发出的**show module**命令将在子类型字段中指示EARL硬件版本。如果Supervisor是EARL 1、1.1或1+,1++，则系统受802.1x漏洞影响。子类型中指示的任何其他EARL版本（如NFFC、NFFC+或NFFC II）不是EARL 1s，不受802.1x漏洞影响。

注意：Supervisor IIG和IIIG不会打印子类型。Supervisor IIG和IIIG是EARL 3，不受802.1x漏洞的影响。

从零件号码表中确定 EARL 版本

模块化 Supervisor Catalyst 5000 系列 Supervisor

主管部件号	管理引擎型号	Earl版本子类型	EARL版本子模型类型	受802.1x漏洞影响
WS-X5005	主管I	EARL 1	WS-F5510	Yes
WS-	主管I	EARL 1	WS-F5510	Yes

X5006				
WS-X5009	主管I	EARL 1	WS-F5510	Yes
WS-X5505	管理引擎II	EARL 1+	WS-F5511	Yes
WS-X5506	管理引擎II	EARL 1+	WS-F5511	Yes
WS-X5509	管理引擎II	EARL 1+	WS-F5511	Yes
WS-X5530-E1	管理引擎III	EARL 1++	WS-F5520	Yes
WS-X5530-E2	管理引擎III NFFC	EARL 2(NFFC)	WS-F5521	无
WS-X5530-E2A	管理引擎III NFFC-A	EARL 2(NFFC)	WS-F5521	无
WS-X5530-E3	管理引擎III NFFC II	EARL 3(NFFC II)	WS-F5531	无
WS-X5530-E3A	管理引擎III NFFC II-A	EARL 3(NFFC II)	WS-F5531	无
WS-X5534	管理引擎III F	EARL 1++	WS-F5520	Yes
WS-X5540	管理引擎II G	EARL 3(NFFC II)	WS-F5531	无
WS-X5550	管理引擎III G	EARL 3(NFFC II)	WS-F5531	无

固定配置 Catalyst 5000 系列交换机

交换机部件号	管理引擎型号	Earl版本子类型	EARL版本子模型类型	受802.1x漏洞影响
WS-C2901	主管I	EARL 1	WS-F5510	Yes
WS-C2902	主管I	EARL 1	WS-F5510	Yes
WS-C2926T	管理引擎II	EARL 1+	WS-F5511	Yes
WS-C2926G	管理引擎II	EARL 1+	WS-F5511	Yes
WS-C2926G	管理引擎III	EARL 3(NFFC)	WS-F5531	无

S	NFFC II	II)		
WS-C2926GL	管理引擎III NFFC II	EARL 3(NFFC II)	WS-F5531	无

注意：在早期软件版本中，EARL 3(NFC II)可称为NFFC+。

通过 SNMP 确定 EARL 版本

EARL 硬件版本可由简单网络管理协议(SNMP)确定。使用
.iso.org.dod.internet.private.enterprises.cisco.workgroup.stack.moduleGrp.mo

duleTable.moduleEntry.moduleSubType

.1.3.6.1.4.1.9.5.1.3.1.1.16

返回值可以是：

- 其他(1)
- empty(2)
- wsf5510(3)(EARL1)
- wsf5511(4)(EARL1+)
- wsx5304(6) (RSM — 未打开SUPERVISOR)
- wsf5520(7)(EARL1++)
- wsf5521(8)(EARL2/NFFC)
- wsf5531(9)(EARL3/NFFCII)

管理引擎II G和III G不会返回值。Supervisor IIG和IIIG是EARL 3，不受802.1x漏洞的影响。

为何只有 Catalyst 5000 EARL 1 版本受影响？

EARL 1版本仅受影响，因为需要为每个保留的MAC地址单独编程EARL 1。所有其他EARL版本都使用范围编程，因此不转发802.1x帧。

如果网络中没有 STP 冗余，是否仍应升级？

当然，Catalyst 5000软件仍在转发所有端口上的数据包。交换机应将这些帧丢弃入站。尽管除非存在STP冗余，否则网络不会出现任何降级，但交换机仍然运行不正确。

802.1x 的漏洞对 Catalyst 4000 和 6000 没有影响

带有EARL 1的Catalyst 5000系列交换机是唯一受影响的交换机。如果交换机位于STP路径中，所有其它交换机将不会转发该帧，实际上会阻止STP环路。

Windows 2000 对 802.1x 的支持

目前，Windows XP(Whistler)是唯一支持802.1x的Microsoft操作系统。据Microsoft称，稍后可能会

通过软件升级或补丁添加Windows 2000的802.1x。目前，Windows XP(Whistler)是唯一支持802.1x的Microsoft操作系统。据Microsoft称，稍后可能会通过软件升级或补丁添加Windows 2000的802.1x。

[相关信息](#)

- [Catalyst 5000 系列软件版本 4.x 发行版本注释](#)
- [技术支持和文档 - Cisco Systems](#)